3.2 DIVISIBILIDAD EN Z^n

3.2.1 Concepto y propiedades básicas

Intuitivamente, podemos entender que dividir el número a por m en Z significa hallar cuantos "pasos" de longitud m debemos recorrer para llegar a a (o en su defecto, a un punto "lo más cercano posible"). Análogamente, la división en Z^n puede suponer el "acercarse" a un punto determinado $\vec{a}$, salvo que entonces necesitamos movernos con n grados de libertad, es decir dando "pasos" según n vectores linealmente independientes. Esto sugiere la siguiente definición:

Sea M una matriz nxn formada por los vectores $\vec{m}_1$, $\vec{m}_2, \ldots,$ $\vec{m}_n$ (2) $\varepsilon\ Z^n$ linealmente independientes, es decir $N = \det(M) \neq 0$, y $\vec{a}$ un vector cualquiera de Z^n. Diremos que M *divide a* $\vec{a}$, denotándolo por $M|\vec{a}$ si y sólo si existe $\vec{x}\ \varepsilon\ Z^n$ tal que

$$\vec{a} = \vec{x}M \qquad (3.11a)$$

es decir
$$\vec{a}M^{-1}\ \varepsilon\ Z^n \qquad (3.11b)$$

Notar que $\vec{x}$ está unívocamente determinado pues $N=\det(M)\neq 0$. Además, cualquier M que cumpla esta condición divide al vector $\vec{0}$, siendo igualmente $\vec{x} = \vec{0}$.

En lo sucesivo, M y N siempre denotarán respectivamente una matriz como la indicada y su determinante. Sin pérdida de generalidad, y para simplificar la nomenclatura, supondremos que $N = \det(M)$ es positivo.

Si en (3.11) hacemos n=1, obtenemos la condición de divisibilidad en Z. En caso contrario, las propiedades de la divisibilidad en Z^n difieren de las conocidas en Z, sobre todo por las dos

---

(2) De ahora en adelante, siempre que hablemos de vectores de Z^n, entenderemos que se trata de vectores fila.

razones siguientes:

(a) En Z, dividendo y divisor son entes iguales, es decir enteros, lo que no ocurre en Z^n.

(b) Z está ordenado pero no así Z^n.

En el siguiente teorema incluimos algunas propiedades básicas de dicho concepto. Como se puede observar, algunas de ellas son totalmente análogas a las propiedades de la divisibilidad en Z. Ver p.e. |A2| ó |NZ1|.

Teorema 3.2.1:

(a) $\forall \vec{a} \in Z^n$, $M|N\vec{a}$ y $M|\vec{a}M$. En particular, si $\vec{a} = \vec{e}_i = (0,\ldots,\overset{(i}{1},\ldots,0)$ nos queda: $M|\vec{m}_i \quad \forall i = 1,\ldots,n$.

(b) Si $M|\vec{a}$ y $M|\vec{b}$ entonces $M|\alpha\vec{a}+\beta\vec{b}$, $\forall \alpha, \beta \in Z$. En particular, $M|\vec{a} \Longrightarrow M|\alpha\vec{a}$.

(c) $\forall \vec{a}$ tal que $M|\vec{a} \Longrightarrow M|\vec{a}A$, siendo A cualquier matriz nxn entera que conmute con M, es decir $AM = MA$.

Las demostraciones son inmediatas a partir de (3.11)

Este concepto de divisibilidad está estrechamente relacionado con el que hubiéramos podido introducir entre las matrices cuadradas enteras. Esto es: $M|A$ si y sólo si existe X tal que $A = XM$, donde ahora M, A y X son matrices nxn enteras y $\det(M) \neq 0$. La relación, fácilmente demostrable, con el concepto estudiado es la siguiente:

Teorema 3.2.2

$M|\vec{a}_i \quad \forall i = 1,\ldots,n$ si y sólo si $M|A$, siendo A la matriz formada por los vectores $\vec{a}_1,\ldots,\vec{a}_n$.

Análogamente a lo que ocurre en Z, dados M y $\vec{v} \in Z^n$ cualesquiera, siempre es posible relacionarlos a través de un "cociente" y un "resto". Veamos un ejemplo: sea M la matriz formada por los vectores $\vec{m}_1 = (3,1)$ y $\vec{m}_2 = (-2,4)$, y $\vec{v} = (10,14)$.

Si $\vec{v}_M$ denota el vector $\vec{v}$ expresado en la base formada por $\vec{m}_1$ y $\vec{m}_2$ tenemos:

$$\vec{v}_M = \vec{v}M^{-1} = (\frac{68}{14}, \frac{32}{14}) \tag{3.12}$$

Separando partes enteras y partes fraccionarias

$$\vec{v}_M = (4,2) + (\frac{12}{14}, \frac{4}{14}) = \vec{q} + \frac{\vec{r}\,'}{N} \tag{3.13}$$

representando ahora $\vec{v}_M$ en la base canónica, nos queda

$$\vec{v} = \vec{v}_M M = \vec{q}M + \frac{\vec{r}\,'}{N}M \tag{3.14}$$

sustituyendo, obtenemos finalmente

$$(10,14) = (4,2)\begin{pmatrix} 3 & 1 \\ -2 & 4 \end{pmatrix} + (2,2) \tag{3.15}$$

donde $\vec{q} = (4,2)$ es el "cociente" y $\vec{r} = (2,2)$ el "resto".

En la figura 3.2.1 ilustramos este ejemplo mostrando el retículo generado por M y como, a través de el, $\vec{v}$ se expresa como suma de los vectores $\vec{q}M$ y $\vec{r}$.

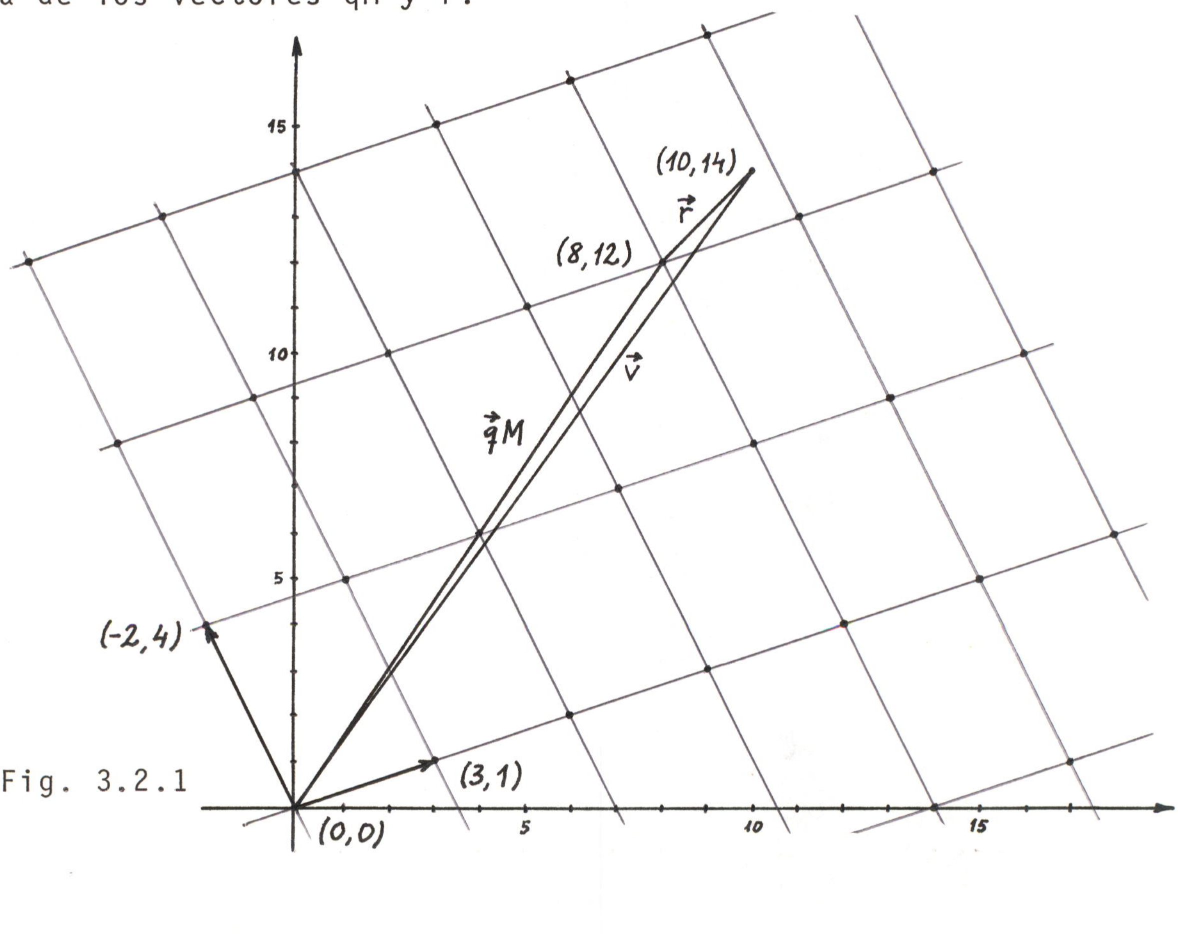

Fig. 3.2.1

En general, tenemos:

Teorema 3.2.3:

Dados M y $\vec{v}$ cualesquiera, N≠0, existen los vectores $\vec{q}$, $\vec{r} \in Z^n$ y $\vec{t} = (t_1,\ldots,t_n) \in Q^n$, $0 \leqslant t_i < 1$, tales que

$$\vec{v} = \vec{q}M + \vec{r} \tag{3.16}$$

donde
$$\vec{r} = \vec{t}M \tag{3.17}$$

Demostración:

El proceso para obtener $\vec{q}$ y $\vec{r}$ es el mismo que el mostrado en el ejemplo y ambos vectores vienen dados por:

$$\vec{q} = E[\vec{v}M^{-1}] \tag{3.18}$$

$$\vec{r} = \{Fr[\vec{v}M^{-1}]\}M \tag{3.19}$$

donde E[ ] y Fr[ ] denotan, respectivamente, parte entera y fraccionaria del vector entre corchetes, es decir de cada una de sus componentes.

¿Cuantos restos distintos se obtienen al dividir por la matriz M?. Sea F el conjunto de puntos en R^n de la forma

$$\vec{t}M = t_1\vec{m}_1 + \ldots + t_n\vec{m}_n \quad \text{con } t_i \in R, \;\; 0 \leqslant t_i < 1 \tag{3.20}$$

Es fácil demostrar que el "paralelotopo" F, llamado en |L1| *dominio fundamental* del retículo generado por M, tesela periódicamente el espacio R^n, es decir, para cada $\vec{x} \in R^n$ existe un y sólo un $\vec{\lambda} \in Z^n$ tal que

$$\vec{x} \in F + \vec{\lambda}M \tag{3.21}$$

Por tanto, el número de puntos reticulares (de coordenadas enteras) en F, o número de posibles restos distintos al dividir por M, debe ser igual al "volumen" de F, es decir, N = det(M).

3.2.2 Máximo común divisor

Si $\vec{v} = (v_1,\ldots,v_n) \varepsilon Z^n$, denotaremos por m.c.d.$\{\vec{v}\}$ o $(\vec{v})$ al máximo común divisor de $v_1,\ldots,v_n$.

Análogamente, si M es una matriz formada por los vectores $\vec{m}_1,\ldots,\vec{m}_n \varepsilon Z^n$,

$$\text{m.c.d.}\{M\} = (M) = ((\vec{m}_1),\ldots,(\vec{m}_n)) \qquad (3.22)$$

Veamos primero un resultado de divisibilidad en Z^n que utiliza el concepto de m.c.d. en Z.

Teorema 3.2.4:

Sean $\vec{a} \varepsilon Z^n$, $\alpha \varepsilon Z$ y M una matriz entera como las consideradas anteriormente. Entonces $M|\alpha\vec{a}$ si y sólo si $M|(N,\alpha)\vec{a}$, con (N,α) = m.c.d.$\{N,\alpha\}$.

Demostración:

La condición suficiente es inmediata pues si $M|(N,\alpha)\vec{a}$ existe $\vec{\lambda}'\varepsilon Z^n$ tal que $(N,\alpha)\vec{a} = \vec{\lambda}'M$, y multiplicando ambos miembros por $\alpha/(N,\alpha)$ obtenemos $\alpha\vec{a} = \vec{\lambda}M$ con $\vec{\lambda} = \frac{\alpha}{(N,\alpha)}\vec{\lambda}'$.

Recíprocamente, si $M|\alpha\vec{a}$, existe $\vec{\lambda} \varepsilon Z^n$ tal que

$$\alpha\vec{a} = \vec{\lambda}M \qquad (3.23)$$

y viene dado por

$$\vec{\lambda} = \alpha\vec{a}M^{-1} = \alpha\vec{a}\frac{M^*}{N} = \alpha'\vec{a}\frac{M^*}{N'} \qquad (3.24)$$

con $\alpha' = \alpha/(N,\alpha)$, $N' = \alpha/(N,\alpha)$, $(\alpha',N') = 1$, y donde $M^* = \left(M_{ji}\right)$ denota la adjunta de la matriz M.

sustituyendo en (3.23)

$$\alpha\vec{a} = \alpha'\vec{\lambda}'M \quad \text{con } \vec{\lambda}' = \vec{a}\frac{M^*}{N'} \varepsilon\, Z^n \tag{3.25}$$

por tanto $\quad (\alpha/\alpha')\vec{a} = (N,\alpha)\vec{a} = \vec{\lambda}'M \Longrightarrow M|(N,\alpha)\vec{a} \qquad (3.26)$

Corolario 3.2.4:

Si $(\alpha,N) = 1$, entonces $M|\alpha\vec{a} \Longleftrightarrow M|\vec{a}$

Para introducir en Z^n una generalización del concepto de "máximo común divisor", recordemos lo que ocurre en Z.

Si a y b son enteros distintos de 0 tales que m.c.d.$\{a,b\}$ = h, pueden expresarse en la forma:

$$a = k_1h, \quad b = k_2h, \quad \text{con } k_1,k_2 \,\varepsilon\, Z, \quad (k_1,k_2) = 1 \tag{3.27}$$

de donde
$$\frac{ak_2}{b} = k_1 \tag{3.28}$$

Por tanto, si α es el menor entero positivo tal que $b|\alpha a$, entonces

$$(a,b) = \frac{|b|}{\alpha} \tag{3.29}$$

Trasladando esta idea a Z^n, tenemos que si α es el menor entero positivo tal que $M|\alpha\vec{a}$, entonces definimos el *máximo común divisor* de $\vec{a}$ y M, denotándolo por m.c.d.$\{\vec{a},M\}$ = $(\vec{a},M)$, como

$$(\vec{a},M) = \frac{\det(M)}{\alpha} = \frac{N}{\alpha} \tag{3.30}$$

Veamos a que equivale (3.30) en Z^2. Sea $\vec{a} = (a_1,a_2)$ y $M = \begin{pmatrix} m_{11} & m_{22} \\ m_{21} & m_{22} \end{pmatrix}$. Buscamos el mínimo $\alpha\varepsilon Z^+$ tal que $M|\alpha\vec{a}$, es decir

$$\alpha\vec{a} = \vec{\lambda}M \quad \text{con } \vec{\lambda} = (\lambda_1,\lambda_2) \,\varepsilon\, Z^2 \tag{3.31}$$

de donde

$$\vec{\lambda} = \alpha\vec{a}M^{-1} \qquad (3.32)$$

desarrollando

$$N(\lambda_1,\lambda_2) = \alpha(a_1m_{22}-a_2m_{21},\ -a_1m_{12}+a_2m_{11}) \qquad (3.33)$$

igualando componentes, se llega a las igualdades:

$$\frac{N}{\alpha} = \frac{a_1m_{22}-a_2m_{21}}{\lambda_1} = \frac{-a_1m_{12}+a_2m_{11}}{\lambda_2} \qquad (3.34)$$

Como α es mínimo, N/α es máximo, por tanto

$$(\vec{a},M) = \frac{N}{\alpha} = \text{m.c.d.}\{N,\ a_1m_{22}-a_2m_{21},\ -a_1m_{12}+a_2m_{11}\} \quad (3.35)$$

En general, y siguiendo el mismo razonamiento, resulta

$$(\vec{a},M) = \frac{N}{\alpha} = \text{m.c.d.}\{N,\ (N\vec{a}M^{-1})\} \qquad (3.36)$$

con $(N\vec{a}M^{-1}) = \text{m.c.d.}\{N\vec{a}M^{-1}\}$.

Notar que, según (3.36), $(\vec{a},M)$ está bien definido en el sentido de que N/α es un entero. Si $n=1$, tenemos $\vec{a} = a \in Z$, $M = m \in Z$ y $M^{-1} = m^{-1}$. Entonces la definición (3.36) coincide con la de m.c.d. en Z.

Sean $\vec{a}_1,\dots,\vec{a}_m$ vectores de Z^n distintos de $\vec{0}$. Definimos el $\text{m.c.d.}\{\vec{a}_1,\dots,\vec{a}_m,M\}$ como $\text{m.c.d.}\{(\vec{a}_1,M),\dots,(\vec{a}_m,M)\}$.

Teorema 3.2.5:

Sean $\vec{a} \in Z^n$ y $\alpha \in Z$ tales que $(\vec{a},M) = 1$ y $(\alpha,N) = 1$. Entonces $(\alpha\vec{a},\ M) = 1$.

Demostración:

$$(\vec{a},M) = (N,\ (N\vec{a}M^{-1})) = 1 \quad \text{y} \quad (N,\alpha) = 1 \qquad (3.37)$$

por tanto,

$$(N,\ \alpha(N\vec{a}M^{-1})) = (N,\ (N\alpha\vec{a}M^{-1})) = (\alpha\vec{a},\ M) = 1 \qquad (3.38)$$

Un resultado análogo al teorema 3.2.4, pero que utiliza el concepto de m.c.d. en Z^n es el siguiente:

Teorema 3.2.6:

Sean $\vec{a} \varepsilon Z^n$ y $\gamma \varepsilon Z$. Entonces $M|\gamma\vec{a}$ si y sólo si $N|\gamma(\vec{a},M)$.

Demostración:

$$M|\gamma\vec{a} \iff \gamma\vec{a}M^{-1} \varepsilon Z^n \iff N|N\gamma\vec{a}M^{-1} \qquad (3.39)$$

es decir, N divide a cada una de las componentes del vector $N\gamma\vec{a}M^{-1}$. Pero $N|N\gamma\vec{a}M^{-1}$ y $N|\gamma N$ si y sólo si

$$N|\gamma(N,(N\vec{a}M^{-1})) \qquad (3.40)$$

lo que equivale a $N|\gamma(\vec{a},M)$.

En particular, si $\gamma=1$,

$$M|\vec{a} \iff N|(\vec{a},M) \qquad (3.41)$$

Considerando conjuntamente los teoremas 3.2.4 y 3.2.6, y tomando $\gamma = \alpha$, obtenemos:

$$M|\alpha\vec{a} \iff M|(N,\alpha)\vec{a} \iff N|\alpha(\vec{a},M) \qquad (3.42)$$

3.3 CONGRUENCIAS EN Z^n

3.3.1 Definición y principales propiedades

Al igual que antes, sea M una matriz formada por los vectores $\vec{m}_1,\ldots,\vec{m}_n \in Z^n$ linealmente independientes. Todos los puntos del espacio R^n que pueden expresarse como combinación lineal de los $\vec{m}_i$ (supondremos en todo caso que la "combinación lineal" es con coeficientes enteros) forman, como es sabido, un retículo.

Diremos que los vectores $\vec{a}$, $\vec{b} \in Z^n$ son *congruentes módulo M*, lo que denotamos por

$$\vec{a} \equiv \vec{b} \pmod{M} \tag{3.43}$$

si y sólo si $M|(\vec{a}-\vec{b})$, es decir, existe $\vec{\lambda} \in Z^n$ tal que

$$\vec{a} - \vec{b} = \vec{\lambda}M \quad \text{ó} \quad \vec{a} = \vec{b} + \vec{\lambda}M \tag{3.44}$$

(o sea, si $\vec{a} - \vec{b}$ pertenece al retículo).

Como antes, si $n=1$, esta definición coincide con la de congruencia en Z.

La congruencia en Z^n es asimismo una relación de equivalencia. En efecto, $\forall\, \vec{a}, \vec{b}, \vec{c} \in Z^n$ se cumple:

1. $\vec{a} \equiv \vec{a} \pmod{M}$ (3.45)
2. $\vec{a} \equiv \vec{b} \pmod{M}$ sii $\vec{b} \equiv \vec{a} \pmod{M}$ (3.46)
3. Si $\vec{a} \equiv \vec{b} \pmod{M}$ y $\vec{b} \equiv \vec{c} \pmod{M}$, entonces
   $\vec{a} \equiv \vec{c} \pmod{M}$ (3.47)

lo cual nos permitirá dividir Z^n en clases de equivalencia.

Por tanto, si $\vec{a} \equiv \vec{b} \pmod{M}$ diremos también que los dos vectores son *iguales módulo M*.

Consecuencias inmediatas de la definición y del teorema 3.2.1 son las siguientes propiedades.

Teorema 3.3.1:

(a) $\vec{m}_i \equiv \vec{0} \pmod{M} \quad \forall i = 1,\ldots,n$ (3.48)

(b) $\forall \vec{a} \in Z^n$, $N\vec{a} \equiv \vec{0} \pmod{M}$ (3.49)

(c) Si $\vec{a} \equiv \vec{b} \pmod{M}$ y $\vec{c} \equiv \vec{d} \pmod{M}$, entonces

$$\alpha\vec{a} + \beta\vec{c} \equiv \alpha\vec{b} + \beta\vec{d} \pmod{M} \ \forall\ \alpha,\beta \in Z \tag{3.50}$$

En particular $\alpha\vec{a} \equiv \alpha\vec{b} \pmod{M}$.

Este último punto implica que las clases de congruencias en Z^n pueden sumarse algebraicamente.

Una afirmación equivalente a (b) es que si $\alpha \equiv \beta \pmod{N}$, entonces

$$\alpha\vec{a} \equiv \beta\vec{a} \pmod{M} \quad \forall\vec{a} \in Z^n \tag{3.51}$$

Otro corolario de este teorema es el que hace referencia a la periodicidad máxima, N, con la que se repiten los puntos, o vectores, congruentes entre sí al "movernos en cualquier dirección de Z^n".

Corolario 3.3.1:

Sean $\vec{a},\vec{b} \in Z^n$ tales que $a_i \equiv b_i \pmod{N}$ $\forall i = 1,2,\ldots,n$. Entonces $\vec{a} \equiv \vec{b} \pmod{M}$.

En efecto, las afirmaciones anteriores son equivalentes a decir que $\forall\vec{k} \in Z^n$, $\vec{a} \equiv \vec{a} + \vec{k}N \pmod{M}$, lo cual es cierto si y sólo si $\vec{k}N \equiv \vec{0} \pmod{M}$ (3.49).

Otro resultado interesante es:

Teorema 3.3.2:

Para cualesquiera $\vec{x}$, $\vec{y} \in Z^n$ y $\alpha,\beta \in Z$, se cumple:

(a) $\alpha\vec{x} \equiv \alpha\vec{y} \pmod{M} \iff (\alpha,N)\vec{x} \equiv (\alpha,N)\vec{y} \pmod{M}$

(b) $\alpha\vec{x} \equiv \beta\vec{x} \pmod{M} \iff \alpha(\vec{x},M) \equiv \beta(\vec{x},M) \pmod{N}$

Demostración:

(a) se deduce directamente del teorema 3.2.4 si hacemos $\vec{a} = \vec{x} - \vec{y}$, y análogamente (b) del teorema 3.2.6 con $\gamma = \alpha - \beta$.

Corolario 3.3.2

(a) Si $\alpha\vec{x} \equiv \alpha\vec{y} \pmod{M}$ y $(\alpha,N) = 1$ entonces $\vec{x} \equiv \vec{y} \pmod{M}$

(b) Si $\alpha\vec{x} \equiv \beta\vec{x} \pmod{M}$ y $(\vec{x},M) = 1$ entonces $\alpha \equiv \beta \pmod{N}$.

Respecto al concepto de congruencia, decimos que las matrices M y M' son *equivalentes* si $\forall\vec{a},\vec{b} \in Z^n$ se cumple

$$\vec{a} \equiv \vec{b} \pmod{M} \iff \vec{a} \equiv \vec{b} \pmod{M'} \qquad (3.52)$$

A la vista de (3.52), esto equivale a decir que ambas matrices generan el mismo retículo. Por tanto, la matriz M formada por los vectores $\vec{m}_1,\ldots,\vec{m}_n$ es equivalente a la matriz M' formada por $\vec{m}'_1,\ldots,\vec{m}'_n$, lo que denotamos por $M \equiv M'$ si

1. Cada $\vec{m}'_i$ es combinación lineal(3) de los $\vec{m}_i$.
2. $\det(M') = \pm\det(M)$ (o cada $\vec{m}_i$ es combinación lineal de los $\vec{m}'_i$).

Por ejemplo, a partir de M obtenemos $M' \equiv M$ si

(a) Cambiamos el orden de los vectores $\vec{m}_i$ o multiplicamos algunos de ellos por -1.

(b) Sumamos a cualquier $\vec{m}_i$ una combinación lineal de los restantes vectores.

3.3.2 Clases residuales

Los vectores $\vec{x}_1,\vec{x}_2,\ldots,\vec{x}_N$ constituyen un *sistema completo de residuos* módulo M si para todo $\vec{y} \in Z^n$ existe un y solamente un $\vec{x}_j$ tal que $\vec{y} \equiv \vec{x}_j \pmod{M}$.

Evidentemente, dada M, existe un número infinito de tales conjuntos. Además, un conjunto de N vectores forman un sistema completo de residuos mod. M si y sólo si no contiene dos vectores que sean congruentes entre sí.

Teorema 3.3.3:

Si $\vec{x} \equiv \vec{y} \pmod{M}$, $\vec{x},\vec{y} \in Z^n$, entonces $(\vec{x},M) = (\vec{y},M)$.

---

(3) Recuérdese que nos referimos a una combinación lineal con coeficientes enteros.

Demostración:

Según la hipótesis, $\vec{x} = \vec{y} + \vec{\lambda}M$, $\vec{\lambda} \in Z^n$, por tanto

$$(\vec{x},M) = (N,(N\vec{x}M^{-1})) = (N,(N[\vec{y}+\vec{\lambda}M]M^{-1})) =$$
$$(N,(N\vec{y}M^{-1} + N\vec{\lambda}MM^{-1})) = (N,(N\vec{y}M^{-1} + N\vec{\lambda})) = (N,(N\vec{y}M^{-1})) = (\vec{y},M)$$

Por otra parte, un *sistema reducido de residuos* módulo M es un conjunto de vectores $\vec{r}_i$ distintos módulo M tales que $(\vec{r}_i,M) = 1$ y todo vector $\vec{x} \in Z^n$, $(\vec{x},M) = 1$ es congruente mod. M con algún miembro $\vec{r}_j$ del conjunto.

En virtud del teorema 3.3.3, es evidente que un sistema reducido de residuos módulo M puede obtenerse a partir de un sistema completo de residuos $\{\vec{x}_i\}$ eliminando aquellos miembros $\vec{x}_k$ tales que $(\vec{x}_k,M) \neq 1$.

Supongamos entonces que en dicho conjunto $\{\vec{x}_i\}$ existe un vector $\vec{x}_j$ tal que $(\vec{x}_j,M) = 1$. Si α y β son enteros distintos módulo N y $(\alpha,N) = (\beta,N) = 1$, por el teorema 3.2.5 resulta que $(\alpha\vec{x}_j,M) = (\beta\vec{x}_j,M) = 1$, y según el teorema 3.3.2(b) $\alpha\vec{x}_j \not\equiv \beta\vec{x}_j \pmod{M}$. De donde, como existen $\phi(N)$[4] números $\alpha_1,\ldots,\alpha_{\phi(N)}$ distintos mod. N y primos relativos con N, un sistema reducido de residuos mod. M tendrá al menos los $\phi(N)$ vectores $\alpha_1\vec{x}_j,\ldots,\alpha_{\phi(N)}\vec{x}_j$ (u otros congruentes con ellos mod. M). Además, como veremos, es fácil demostrar que no existen otros. Por tanto si, dada M, existe un sistema reducido de residuos módulo M, este consta de $\phi(N)$ vectores.

El siguiente teorema nos permite obtener clases residuales completas y reducidas a partir de otras dadas.

---

(4) ϕ es la "función de Euler" o "totient". Ver p.e. |A2| o |NZ1|.

Teorema 3.3.4:

Sea $S=\{\vec{x}_1,\ldots,\vec{x}_m\}$ un sistema completo de residuos mod.M. Para cualesquiera $\vec{v}\in Z^n$ y $\alpha\in Z$, $(\alpha,N) = 1$, los conjuntos $S+\vec{v} = \{\vec{x}_1+\vec{v},\ldots,\vec{x}_m+\vec{v}\}$ y $\alpha S = \{\alpha\vec{x}_1,\ldots,\alpha\vec{x}_m\}$ también son sistemas completos de residuos. Además, si S es un sistema reducido de residuos mod. M, αS también lo es.

Demostración:

Los conjuntos $S+\vec{v}$ y αS constan del mismo número de elementos que S , por tanto basta demostrar que, si $i \neq j$

$$\vec{x}_i + \vec{v} \not\equiv \vec{x}_j + \vec{v} \pmod{M} \qquad (3.53)$$

$$y \quad \alpha\vec{x}_i \not\equiv \alpha\vec{x}_j \pmod{M} \qquad (3.54)$$

lo cual se cumple pues, razonando por contradicción, (3.53) es consecuencia inmediata del teorema 3.3.1(c) y (3.54) del corolario 3.3.2(a).

Por otra parte, según el teorema 3.2.5, si $(\vec{x}_i,M) = 1$ y $(\alpha,N) = 1$ resulta $(\alpha\vec{x}_i,M) = 1$, lo que demuestra la última parte del teorema.

3.3.3 Teselación de R^n

Sea $\{\vec{r}_1,\ldots,\vec{r}_N\}$ un sistema completo de residuos mod. M. Entonces el conjunto $C_{\vec{0}}$ de n-cubos unitarios con centros $\vec{r}_1,\ldots,\vec{r}_N$ tesela periódicamente, mediante traslaciones, el espacio R^n.

En efecto, a partir de $C_{\vec{0}}$ definimos los conjuntos

$C_{\vec{a}}$ = {n-cubos unitarios con centros $\vec{s}_i \mid \vec{s}_i = \vec{r}_i+\vec{a}M$, $\vec{a}\in Z^n$, $i=1,\ldots,N$}.

Entonces nos basta comprobar que todo vector $\vec{x}\in Z^n$ pertenece a un conjunto $C_{\vec{a}}$ y sólo a uno.

Dado $\vec{x}$, y por ser $\{\vec{r}_1,\ldots,\vec{r}_N\}$ un sistema completo de residuos, existe un $\vec{r}_i$, y sólo uno, tal que $\vec{r}_i \equiv \vec{x} \pmod{M}$. Es decir, existe $\vec{\lambda}$ tal que $\vec{r}_i - \vec{x} = \vec{\lambda}M$, de donde

$$\vec{x} = \vec{r}_i + (-\vec{\lambda})M \in C_{\vec{a}} \tag{3.55}$$

con $\vec{a} = -\vec{\lambda}$. Además, teniendo en cuenta que $\det(M) \neq 0$, se obtiene que $\vec{a}$ viene dado unívocamente por

$$\vec{a} = -\vec{\lambda} = (\vec{x} - \vec{r}_i)M^{-1} \tag{3.56}$$

En el caso n=2, cada conjunto $C_{\vec{a}}$, $\vec{a} \in Z^2$ está formado por N cuadrados de lado unidad cuyos centros corresponden a N vectores del plano distintos entre sí mod. M.

Entonces, siguiendo con el ejemplo del apartado 3.2.1, $M = \begin{pmatrix} 3 & 1 \\ -2 & 4 \end{pmatrix}$, N = 14, y eligiendo los vectores $\vec{r}_1 = (r_{11}, r_{12}), \ldots, \vec{r}_N = (r_{N1}, r_{N2})$ de manera que sus componentes sean no negativas y la suma $r_{i1}+r_{i2}$ sea mínima para cada i = 1,...,N (en la sección 4 justificaremos esta elección), $C_{\vec{0}}$ es el lugar geométrico en forma de "L" que tesela o "embaldosa" el plano según se muestra en la figura 3.3.1.

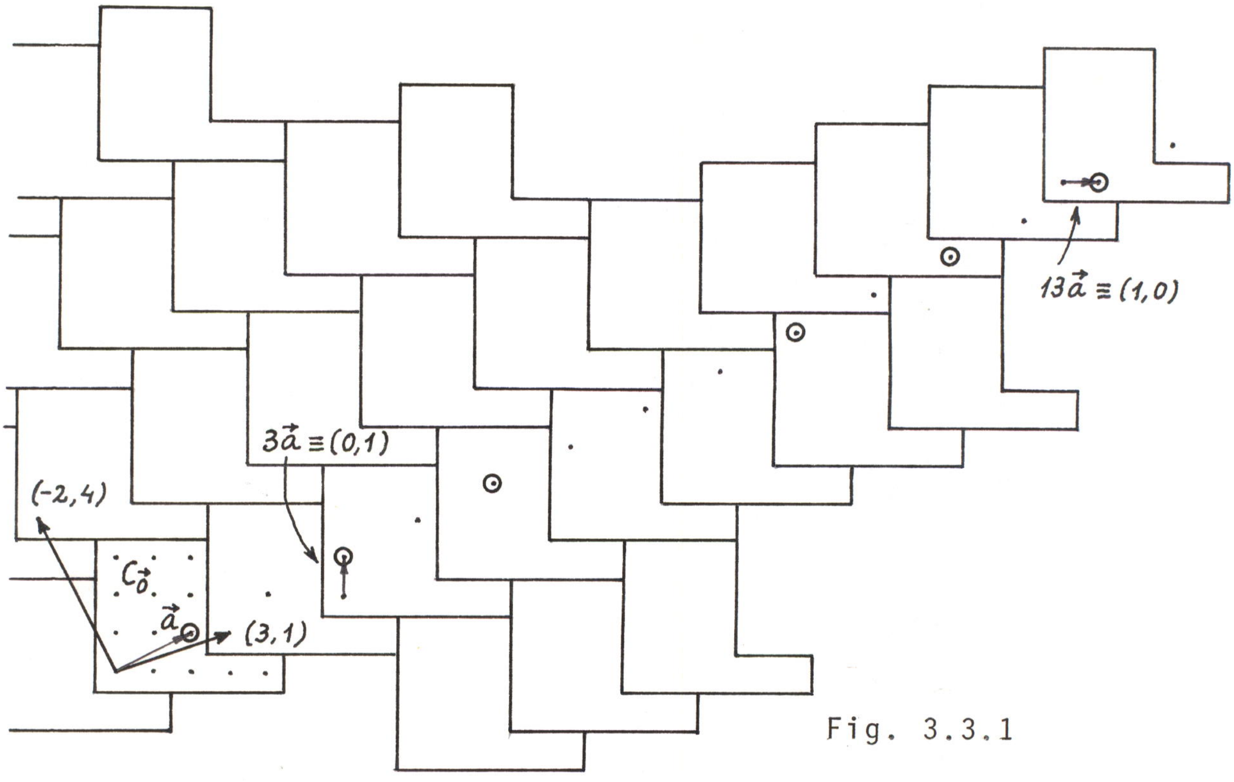

Fig. 3.3.1

3.3.4 Grupos

El conjunto de vectores de Z^n módulo M (o, más propiamente, el conjunto de clases residuales en Z^n mod. M) junto con la operación suma tiene estructura de *grupo abeliano.*

En efecto, la suma de vectores mod. M es cerrada, asociativa y conmutativa. Además, existe elemento neutro:el vector $\vec{0}$; y cada vector $\vec{a}$ tiene inverso: $-\vec{a}$ (mod M). A este grupo aditivo, cuyo orden es N = det(M), lo denotaremos por A_M.

Evidentemente, los vectores coordenados unitarios $\vec{e}_1,\ldots,\vec{e}_n$ constituyen un conjunto de generadores de A_M con independencia de M. En particular, si n=1, dicho conjunto contiene un sólo elemento:el 1. Por tanto, y como sabemos, en este caso el grupo A_M (ahora M es un entero) es siempre cíclico.

Sin embargo, cuando n>1 esto no es cierto, lo que sugiere el problema de averiguar que condiciones debe cumplir M para que A_M sea cíclico.

Veamos primero que elementos generan por sí solos A_M.

Teorema 3.3.5:

El vector $\vec{a} \in Z^n$ (propiamente, la clase residual que representa) genera el grupo A_M si y sólo si $(\vec{a},M) = 1$.

Demostración:

Que la condición es necesaria es consecuencia directa de los conceptos implicados: el de generador y el de m. c. d.

En cuanto a que la condición es suficiente, basta notar que $(\vec{a},M) = 1$ implica que todos los vectores $\vec{a}$, $2\vec{a},\ldots$, $N\vec{a}$ son distintos módulo M. De lo contrario, existirían enteros i y j tales que

$$i\vec{a} \equiv j\vec{a} \pmod{M}, \qquad 0 \leqslant i < j \leqslant N \tag{3.57}$$

de donde, según el corolario 3.3.2(b)